



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/735,215	12/11/2000	David Michael Kurn	20206-038 (P00-3420)	4261

7590 11/18/2004

Bill Streeter
HEWLETT-PACKARD COMPANY
Intellectual Property Administration
P.O. Box 272400
Fort Collins, CO 80527-2400

EXAMINER

CHAI, LONGBIT

ART UNIT	PAPER NUMBER
----------	--------------

2131

DATE MAILED: 11/18/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

09/735,215

Applicant(s)

KURN, DAVID MICHAEL

Examiner

Longbit Chai

Art Unit

2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 22 September 2004.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-10 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-10 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 4/30/2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. _____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1 – 10 have been presented for examination. Claims 5 and 6 have been amended and new claims 9 and 10 have been added in an amendment filed 09/22/2004. Claims 1 – 10 have been examined.

Response to Arguments

2. Applicant's arguments with respect to the claims 1 – 7 have been considered but are not persuasive.

3. Applicant asserts that Hardjono or Bellare (individually or in combination) fails to disclose "how to update a master key by a server and by requiring only some passwords to be revealed". However, Examiner notes that Hardjono is relied upon for providing the logic by dividing the master key into N shares (or secrets) and then using threshold encryption scheme such that any M of the shares (M less than or equal to N) can be used to construct the master key in a multicast server and clients environment.

4. Examiner further notes that Bellare is relied upon for teaching a method "password-based encryption mechanism" to encrypt the shares (or secrets) by a password-derived key and thereby passwords are required to decrypt / encrypt the secrets. As a result, the master key can be updated and reconstructed by requiring only some passwords to be revealed (from the clients) so that the corresponding shares (or secrets) can be obtained (M less than or equal to N) and the threshold encryption scheme can then be applied as taught by Hardjono.

Priority

5. No claim for priority has been made in this application.
6. The effective filing date for the subject matter defined in the pending claims in this application is 12/11/2000.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

1. Claims 1, 2, 5 and 6 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (Patent Number: US 6182214 B1), hereinafter referred to as Hardjono, in view of Bellare (Proposal for P1363 Study Group on Password-Based Authenticated-Key-Exchange Methods), hereinafter referred to as Bellare.

2. As per claims 1, 5 and 8, Hardjono teaches a cryptographic system in a computer system, comprising:

- a. at least one server (Hardjono: see for example, Figure 1); and
- b. at least one secret value including a master key, the master key being split into two or more parts wherein fewer than all the parts are required for reassembling the master key (Hardjono: see for example, Column 2 Line 11 – 20 and Column 5 Line 50 – 65),

3. Hardjono teaches the parts are further encrypted (Hardjono: see for example, Column 6 Line 15 – 16).
4. Hardjono does not expressly teach the parts being encrypted by a password-derived or token-based key.
5. Bellare teaches the parts being encrypted by a password-derived key (Bellare: see for example, section of problem description).
6. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Bellare within the system of Hardjono because (a) many common cryptographic methods for authentication require large, random high-grade secret keys, yet, the secrets that human beings can conveniently memorize and reliably reproduce tend to be low-grade secrets, and (b) Bellare discloses password-based authentication technique that offers very strong guarantees using a very simple trust model based on a weak authenticator and this trust model is in fact the predominant trust model used in person-to-computer authentication.
7. Hardjono as modified further teaches:
 - c. the parts being encrypted by a password-derived or token-based key, each part being associated with a password wherein the at least one server can update the master key by requiring only some of the passwords to be revealed (Hardjono: see for example, Column 6 Line 14 and Column 6 Line 19 – 20).
8. As per claims 2 and 6, Hardjono as modified teaches the claimed invention as described above (see claim 1). Hardjono as modified further teaches the master key is

used for protecting sensitive information processed by the at least one server
(Hardjono: see for example, Column 1 Line 28 – 30).

9. Claim 3 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (Patent Number: US 6182214 B1), hereinafter referred to as Hardjono, in view of Newton (Patent Number: 5771291), hereinafter referred to as Newton.

10. As per claim 3, Hardjono as modified teaches the claimed invention as described above (see claim 1). Hardjono as modified does not teach the sensitive information is stored in the database.

11. Newton teaches the sensitive information is stored in the database (Newton: see for example, Column 6 Line 26 – 31).

12. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Newton within the system of Hardjono because Newton discloses an effective security system using database of storing and accessing sensitive information (Newton: see for example, Column 1 Line 67 and Column 6 Line 26 – 31).

13. Claims 4 and 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hardjono (Patent Number: US 6182214 B1), hereinafter referred to as Hardjono, in view of Denning (Descriptions of Key Escrow Systems), hereinafter referred to as Denning.

Art Unit: 2131

14. As per claims 4 and 7, Hardjono as modified teaches the claimed invention as described above (see claim 1). Hardjono as modified does not teach the master key is split into the two or more parts according to the Bloom-Shamir methodology.

15. Denning teaches the master key is split into the two or more parts according to the Bloom-Shamir methodology (Denning: see for example, section of RSA Secure and subsection of Key Escrow Component).

16. It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Denning within the system of Hardjono because Denning discloses the master key is generated and stored in escrow and is split with a "k out of n" threshold scheme using Bloom-Shamir secret sharing techniques (Denning: see for example, section of RSA Secure and subsection of Key Escrow Component).

17. As per claim 9, Hardjono as modified teaches the claimed invention as described above (see claim 8). Hardjono as modified further teaches comprising an input coupled to the means for updating the master key, the input receiving some of the passwords (See the same rationale applied herein as above in rejecting claim 8, which recites the parts being encrypted by a password-derived key and thereby the encryption / decryption function can't be proceeded without passwords).

18. As per claim 10, Hardjono as modified teaches the claimed invention as described above (see claim 9). Hardjono as modified further teaches some of the

passwords are received from a plurality of clients coupled to the server (See the same rationale applied herein as above in rejecting claim 8 and multicast server and clients as taught by Hardjono shown in Figure 1).

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2131


Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 703-305-0710. The examiner can normally be reached on Monday-Friday 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R Sheikh can be reached on 703-305-9648. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC


AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100